

## CLAIMS

What is claimed is:

1. A method of secure communication, comprising:
  2. receiving a request for a data transaction from a client lacking hardware cryptography functionality, together with security parameters specific to the client, at a server through a secure connection between the client and the server;
  5. performing any necessary security processing for the requested data transaction within the server on behalf of the client utilizing hardware cryptography functionality available within the server; and
  8. after performing any necessary security processing on the requested data transaction, forwarding the processed data transaction to a target of the requested data transaction as if originating from the client.
1. The method of claim 1, wherein the step of receiving a request for a data transaction from a client lacking hardware cryptography functionality, together with security parameters specific to the client, at a server through a secure connection between the client and the server further comprises:
  5. receiving the requested data transaction through an IPSEC connection.
1. The method of claim 1, wherein the step of receiving a request for a data transaction from a client lacking hardware cryptography functionality, together with security parameters specific to the client, at a server through a secure connection between the client and the server further comprises:
  5. receiving encryption keys or a digital certificate assigned to the client.

1       4. The method of claim 1, wherein the step of performing any necessary security  
2       processing for the requested data transaction within the server on behalf of the client utilizing  
3       hardware cryptography functionality available within the server further comprises:  
4             encrypting data within the requested data transaction; or  
5             generating a digital signature for attachment to the data transaction.

1       5. The method of claim 1, wherein the step of forwarding the processed data transaction  
2       to a target of the requested data transaction as if originating from the client further comprises:  
3             forwarding the processed data transaction via an SSL transaction.

1       6. The method of claim 1, further comprising:  
2             receiving a response to the processed data transaction at the server;  
3             performing any security processing required by the response; and  
4             forwarding the processed response, together with any results of the security  
5       processing, to the client via the secure connection.

1       7. The method of claim 6, wherein the step of performing any security processing  
2       required by the response further comprises:  
3             decrypting the received response; or  
4             validating a digital signature attached to the received response.

1       8. A system for secure communication, comprising:  
2           a client lacking hardware cryptography functionality;  
3           a server including hardware cryptography functionality;  
4           a secure Internet Protocol connection between the client and the server;  
5           means for receiving a request for a data transaction from the client, together with  
6           security parameters specific to the client, at the server through the secure connection;  
7           means for performing any necessary security processing for the requested data  
8           transaction within the server on behalf of the client utilizing the hardware cryptography  
9           functionality available within the server; and  
10           means, responsive to completion of performing any necessary security processing on  
11           the requested data transaction, for forwarding the processed data transaction to a target of the  
12           requested data transaction as if originating from the client.

1       9. The system of claim 8, wherein secure connection further comprises:  
2           an IPSEC connection.

1       10. The system of claim 8, wherein the means for receiving a request for a data  
2           transaction from the client, together with security parameters specific to the client, at the  
3           server through the secure connection further comprises:  
4           means for securely receiving encryption keys or a digital certificate assigned to the  
5           client.

1       11. The system of claim 8, wherein the means for performing any necessary security  
2       processing for the requested data transaction within the server on behalf of the client utilizing  
3       hardware cryptography functionality available within the server further comprises:  
4           means for encrypting data within the requested data transaction; or  
5           means for generating a digital signature for attachment to the data transaction.

1       12. The system of claim 8, wherein the means for forwarding the processed data  
2       transaction to a target of the requested data transaction as if originating from the client  
3       further comprises:  
4           means for forwarding the processed data transaction via an SSL transaction.

1       13. The system of claim 8, further comprising:  
2           means for receiving a response to the processed data transaction at the server;  
3           means for performing any security processing required by the response; and  
4           means for forwarding the processed response, together with any results of the security  
5       processing, to the client via the secure connection.

1       14. The system of claim 13, wherein the means for performing any security processing  
2       required by the response further comprises:  
3           means for decrypting the received response; or  
4           means for validating a digital signature attached to the received response.

1       15. A computer program product within a computer usable medium for secure  
2       communication, comprising:

3                 instructions for receiving a request for a data transaction from a client lacking  
4       hardware cryptography functionality, together with security parameters specific to the client,  
5       at a server through a secure connection between the client and the server;

6                 instructions for performing any necessary security processing for the requested data  
7       transaction within the server on behalf of the client utilizing hardware cryptography  
8       functionality available within the server; and

9                 instructions, responsive to completion of performing any necessary security  
10      processing on the requested data transaction, for forwarding the processed data transaction  
11      to a target of the requested data transaction as if originating from the client.

1       16. The computer program product of claim 15, wherein the instructions for receiving a  
2       request for a data transaction from a client lacking hardware cryptography functionality,  
3       together with security parameters specific to the client, at a server through a secure  
4       connection between the client and the server further comprise:

5                 instructions for receiving the requested data transaction through an IPSEC  
6       connection.

1       17. The computer program product of claim 15, wherein the instructions for receiving a  
2       request for a data transaction from a client lacking hardware cryptography functionality,  
3       together with security parameters specific to the client, at a server through a secure  
4       connection between the client and the server further comprise:

5                 instructions for securely receiving encryption keys or a digital certificate assigned to  
6       the client.

1       18. The computer program product of claim 15, wherein the instructions for performing  
2       any necessary security processing for the requested data transaction within the server on  
3       behalf of the client utilizing hardware cryptography functionality available within the server  
4       further comprise:

- 5              instructions for encrypting data within the requested data transaction; or  
6              instructions for generating a digital signature for attachment to the data transaction.

1       19. The computer program product of claim 15, wherein the instructions for forwarding  
2       the processed data transaction to a target of the requested data transaction as if originating  
3       from the client further comprises:

- 4              instructions for forwarding the processed data transaction via an SSL transaction.

1       20. The computer program product of claim 15, further comprising:

- 2              instructions for receiving a response to the processed data transaction at the server;  
3              instructions for performing any security processing required by the response; and  
4              instructions for forwarding the processed response, together with any results of the  
5       security processing, to the client via the secure connection.

1       21. The computer program product of claim 20, wherein the instructions for performing  
2       any security processing required by the response further comprise:

- 3              instructions for decrypting the received response; or  
4              instructions for validating a digital signature attached to the received response.